<u>WHAT IS CLAIMED IS:</u>

1   1.   A secure passcode authentication system, the system comprising:

2   an Access Control Server (ACS) configured to receive a request for passcode

3 authentication of a Primary Account Number (PAN), and configured to request a passcode

4 corresponding to the PAN;

5   a front end Hardware Security Module (HSM) coupled to the ACS, and

6 configured to receive the passcode and generate an encrypted passcode using a local encryption

7 key; and

8   a back end HSM configured to receive the encrypted passcode from the front end

9 HSM and further configured to recover a clear form of the passcode, generate a back end

10 encrypted passcode, and communicate the back end encrypted passcode to an authentication

11 network.

1   2.   The system of Claim 1, wherein the request for passcode authentication

2 comprises a request for a Personal Identification Number (PIN) authentication.

1   3.   The system of Claim 1, wherein the ACS is further configured to receive

2 an authentication message from the authentication network.

1   4.   The system of Claim 1, wherein the ACS is further configured to generate

2 a unique transaction identification and include the unique transaction identification as a hidden

3 field in the request for the passcode.

1   5.   The system of Claim 4, wherein the front end HSM is configured to

2 generate a hash value based in part on the unique transaction identification, and wherein the ACS

3 is configured to include the hash value as an additional hidden field in the request for the

4 passcode.

1   6.   The system of Claim 1, wherein the request for the passcode includes an

2 instruction to direct the passcode to the front end HSM.

1   7.   The system of Claim 1, wherein the front end HSM comprises a software

2 HSM.

1   8.   The system of Claim 1, wherein the front end HSM comprises a hardware

2 HSM.

1   9.   The system of Claim 1, wherein the front end HSM is configured to

2 receive the passcode in a first encrypted format.

1   10.   The system of Claim 9, wherein the first encrypted format comprises a

2 Secure Sockets Layer (SSL) encrypted format.

1   11.   The system of Claim 1, wherein the front end HSM is configured to

2 receive a cardholder encrypted passcode from the ACS.

1   12.   The system of Claim 1, wherein the front end HSM is configured to

2 receive a cardholder encrypted passcode from a cardholder device.

1   13.   The system of Claim 1, wherein the back end HSM is configured to

2 generate the back end encrypted passcode by generating a PINBLOCK using the clear form of

3 the passcode and encrypting the PINBLOCK using an Acquirer Working Key (AWK).

1   14.   The system of Claim 1, wherein the authentication network comprises an

2 Internet Payment Gateway Server (IPGS).

1   15.   The system of Claim 14, wherein the authentication network further

2 comprises an issuer server coupled to the IPGS.

1   16.   A secure passcode authentication system, the system comprising:

2   an Access Control Server (ACS) configured to receive a request for Personal

3 Identification Number (PIN) authentication of a Primary Account Number (PAN), and

4 configured to generate a request for a PIN corresponding to the PAN, the request for the PIN

5 including hidden fields comprising a unique transaction identifier and a hash value;

6   a front end Hardware Security Module (HSM) coupled to the ACS, and

7 configured to generate the hash value based in part on the unique transaction identifier, and

8 further configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the

9 PIN, and generate a local encrypted PIN using a local encryption key; and

25

10   a back end HSM configured to receive the local encrypted PIN from the front end

11 HSM and further configured to recover a clear form of the PIN from the local encrypted PIN,

12 generate an Acquirer Working Key (AWK) encrypted PIN, and communicate the AWK

13 encrypted PIN to an authentication network.

1   17. The system of Claim 16, wherein the front end HSM generates the local

2 encrypted key using a triple DES algorithm.

1   18. A secure passcode authentication system, the system comprising:

2   an Access Control Server (ACS) configured to receive a request for Personal

3 Identification Number (PIN) authentication of a Primary Account Number (PAN), and

4 configured to generate a request for a PIN corresponding to the PAN, the request for the PIN

5 including an instruction to provide the PIN to a destination address; and

6   a front end Hardware Security Module (HSM) having said destination address and

7 coupled to the ACS, and configured to receive an encrypted PIN, decrypt the PIN to recover a

8 clear form of the PIN, and generate an Acquirer Working Key (AWK) encrypted PIN using an

9 AWK encryption key, and configured to communicate the AWK encrypted PIN to an

10 authentication network.

1   19. A method for providing secure passcode authentication, the method

2 comprising:

3   requesting a Personal Identification Number (PIN) corresponding to a Primary

4 Account Number (PAN);

5   receiving the PIN in response to the request;

6   generating a PINBLOCK based in part on the PIN;

7   encrypting the PINBLOCK using a local key in a front end Hardware Security

8 Module (HSM) to generate a local key encrypted PINBLOCK;

9   decrypting the local key encrypted PINBLOCK with a back end HSM;

10   generating a back end encrypted PIN with the back end HSM;

11   communicating the back end encrypted PIN to an authentication network; and

12   receiving an authentication response from the authentication network.

1   20. The method of Claim 19, wherein requesting the PIN comprises:

2   generating a unique transaction identifier;

3   generating a hash value with the front end HSM based in part on the unique

4   transaction identifier;

5   generating a query having the unique transaction identifier and hash value as

6   fields in the query; and

7   communicating the query.

1   21.   The method of Claim 19, wherein requesting the PIN comprises:

2   generating a query having an instruction directing a query response be directed to

3   a destination address corresponding to the front end HSM; and

4   communicating the query over an Internet connection to a cardholder device.

1   22.   The method of Claim 19, wherein receiving the PIN comprises receiving a

2   Secure Sockets Layer (SSL) encrypted PIN.

1   23.   The method of Claim 22, wherein receiving the PIN further comprises

2   receiving the SSL encrypted PIN at an Access Control Server (ACS).

1   24.   The method of Claim 22, wherein receiving the PIN further comprises

2   receiving the SSL encrypted PIN from a cardholder device at the front end HSM.

1   25.   The method of Claim 19, wherein the front end HSM comprises a

2   software HSM implementation within an Access Control Server (ACS).

1   26.   The method of Claim 19, wherein encrypting the PINBLOCK comprises

2   encrypting the PINBLOCK using a triple DES encryption algorithm.

1   27.   The method of Claim 19, wherein generating the back end encrypted PIN

2   comprises:

3   generating a back end PINBLOCK from a clear form of the PIN; and

4   encrypting the PIN with the back end HSM using an Acquirer Working Key

5   (AWK).

1   28.   A method for providing secure passcode authentication, the method

2   comprising:

3   receiving an encrypted Personal Identification Number (PIN) corresponding to a

4   Primary Account Number (PAN);

5   decrypting the encrypted PIN in a front end Hardware Security Module (HSM) to

6   generate a clear form of the PIN;

7   generating a PINBLOCK based in part on the clear form of the PIN;

8   generating in a back end HSM a back end encrypted PIN based in part on the

9   PINBLOCK;

10   communicating the back end encrypted PIN to an authentication network; and

11   receiving an authentication response from the authentication network.

1   29.   The method of Claim 28, wherein the front end HSM comprises the back

2   end HSM.

1   30.   The method of Claim 28, wherein receiving the encrypted PIN comprises

2   receiving a Secure Sockets Layer (SSL) encrypted PIN over an Internet connection from a

3   cardholder device.

1   31.   The method of Claim 28, wherein generating the back end encrypted PIN

2   comprises generating an Acquirer Working Key (AWK) encrypted PIN.

1   32.   A method for providing secure passcode authentication, the method

2   comprising:

3   generating encryption data;

4   querying a cardholder for a Personal Identification Number (PIN) corresponding

5   to a Primary Account Number (PAN);

6   receiving an encrypted PIN and at least a portion of the encryption data in

7   response to the query;

8   generating a clear form of the PIN based in part on the encrypted PIN;

9   generating a PINBLOCK based in part on the clear form of the PIN;

10   encrypting the PINBLOCK in a front end Hardware Security Module (HSM)

11   using triple DES encryption to generate an encrypted PIN (EPIN);

12   decrypting the EPIN in a back end HSM to recover the clear form of the PIN;

13   encrypting the clear form of the PIN in the back end HSM using an Acquirer

14 Working Key (AWK) to generate an AWK encrypted PIN;

15   communicating the AWK encrypted PIN to an authentication network; and

16   receiving an authentication response.